## REMARKS

For the present Response, claims 1, 4, 6-10, 14, 17, 19-23, 27, 30, and 32-36 remain pending.

**Claim Rejections Under 35 U.S.C. § 103**

Claims 1, 4, 6-10, 14, 17, 19-23, 27, 30, and 32-36 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 6,424,654, issued to Daizo (*Daizo* hereinafter), in view of "Authentication of DHCP Messages" issued to Droms et al. (*Droms* hereinafter), and in further view of U.S. Pat. No. 5,884,024, issued to Lim et al. (*Lim* hereinafter). Applicants respectfully traverse the foregoing rejections for the following reasons.

Applicants' proposed invention employs a server checker client that draws (via configuration request broadcast) configuration server responses which are then analyzed to detect unauthorized servers, which are subsequently individually targeted (by unicasting) with configuration requests to occupy the unauthorized servers and prevent them from interacting with the network clients.

Regarding the grounds for rejecting independent claims 1, 14 and 27 cited by reference item 8 on page 2 of the Office Action, Applicants disagree that *Daizo* teaches a method for preventing unauthorized dynamic host configuration servers from responding to client configuration requests. *Daizo* discloses a method and system for reducing the complexity of IP address allocation in a multi-DHCP server environment by selecting and associating a specified DHCP server with each client. Included in *Daizo's* disclosure is a description of the well-known host configuration procedure whereby a DHCP client receives configuration offer messages from DHC servers responding to the client broadcasting a host configuration request. Nothing in *Daizo* relates directly or indirectly to detecting and/or responding to unauthorized DHCP servers.

Regarding the grounds for rejecting claims 1, 14, and 27 cited by reference item 10 on page 3, Applicants agree that *Droms* discloses a method for authenticating DHCP messages and the sources of DHCP messages. However, neither the "Protocol 0" nor "Protocol 1" technique described at page 3 *et seq.*, authenticate the server using server identification data, or, more specifically, server identification data contained within configuration offer messages received by a checker client from the DHC servers. The "Protocol 0" depicted in section 3, pg. 3- pg. 4, is

described as a simple, constant authentication token known (i.e. pre-specified) to both the client and server that provides mutual authentication. The token therefore is neither client-centric nor server-centric. Nothing in the described "Protocol 0" relates to processing of configuration offer messages, or more specifically, to server-specific identification data within configuration offer messages received from DHCP servers.

The Protocol 1 technique described at page 4 *et seq.*, employs an authentication mechanism wherein the client receives a DHCP offer message that include authentication information. In contrast to the proposed invention recited in Applicants' independent claims, however, the authentication is based on encryption of a secret shared between the server and client (see pg. 4, section 4, pg. 5, section 4.1) and not on the identity of the DHCP server per se. Thus, Applicants disagree that *Droms* discloses detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages.

Regarding reference item 12 on pages 3-4 of the Office Action, Applicants contend that *Lim* fails to disclose unicasting host configuration requests from said server checker client to said unauthorized dynamic configuration server in response to detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages. Furthermore, since *Droms* fails to disclose detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages, even in combination, *Lim* and *Droms* do not disclose this limitation.

Applicants further disagree with the assertion in reference item 13 on page 4 of the Office Action that the disclosure of *Droms* at page 2 provides motivation to combine the "IP address hogging" problem cited by *Lim* as a remedial feature of any kind. Similar to *Lim*, *Droms* describes IP address hogging as a problem and not a remedial feature to be used to "silence" an unauthorized DHCP server with respect to non-checker clients.

For the foregoing reasons, Applicants submit that claims 1, 14, and 27, and all claims depending therefrom are patentably distinct from *Daizo*, *Droms*, and *Lim*, individually or in any combination. It is respectfully submitted that the pending claims are in condition for allowance and favorable action is requested. No extension of time is believed to be required. However, in

the event that an extension of time is required, please charge that extension fee and any other required fees to **IBM Corporation Deposit Account Number 09-0457.**

Applicant invite the Examiner to contact the undersigned attorney of record at (512) 343-6116 if such would further or expedite the prosecution of the present application.

Respectfully submitted,

Matthew W. Baca
*Reg. No. 42,277*
DILLON & YUDELL LLP
8911 North Capital of Texas Highway
Suite 2110
Austin, Texas 78759
Telephone 512-343-6116
Facsimile 512-343-6446

ATTORNEY FOR APPLICANTS